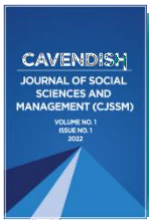
Journal of Social Sciences and Management



Electronic Businesses Development and its Associate Cybercrimes: An Assessment of Financial Technology Utilisation in Nigeria

CJSSM
ISSN 2518-8623

Volume 2. Issue I
pp. 1-16, June 2023
www.cavendish.ac.ug
email: secretarycjssm@cavendish.ac.ug

Jacob Eneji Ashibi
National Open University of Nigeria
Email: eashibi@noun.edu.ng

Akoji Ocheja
National Open University of Nigeria
Email: aocheja@noun.edu.ng

Vitalis Odinaka Ugwukwu
National Open University of Nigeria
Email: vugwukwu@noun.edu.ng

How to cite this article: *Ashibi, J. E, Ocheja, A & Ugwukwu, V. O. (2023). Electronic Businesses Development and its Associate Cybercrimes: An Assessment of Financial Technology Utilisation in Nigeria. Cavendish Journal of Social Science and Management, Vol 2.*

Abstract

The proliferation of financial technologies has contributed immensely to the growth and development of electronic businesses in Nigeria. However, many users are apprehensive due to emerging trends of cybercrimes associated with the utilisation of financial technologies for business transactions. The study examines electronic businesses and its associate cybercrimes in Nigeria. It employs the quantitative design, utilising the questionnaire as the major instrument of data collection. Twenty-three (23) electronic businesses and consumers of financial technologies were randomly selected for the study. The snowball and purposive sampling techniques were also utilized in administering the research instruments. Data obtained for the study were analysed using the Statistical Package for the Social Sciences (SPSS) to determine commonalities and patterns in the respondents' responses. Emerging cybercrimes were found to have adverse effects on the development of electronic businesses. The study recommends awareness campaigns to up consumers' financial technology literacy; adequate policy formulation and enforcement to punish and deter potential cybercriminals; and the Central Bank of Nigeria (CBN) should strive for policies that will compel financial institutions to upgrade their financial gateways to incorporate Europay, MasterCard and Visa (EMV) Chip and Near Field Communication (NFC) technologies to prevent fraudulent transactions and boost consumers' confidence.

Key words: *Electronic Business, Cybercrime, Financial fraud, financial technologies*

Introduction

Before the 19th century, commercial enterprises or businesses in Nigeria were largely transacted in the physical space, where both merchants and their customers converge, initiate a bargain and settle for the exchange of goods and services. This physical approach to commerce was not only time-consuming but also tasking due to its rigorous processes, especially for merchants and customers to meet and settle for a common exchange. Merchants had no other option other than to move their goods and services to designated areas commonly referred to as a Market places, where customers must also physically visit to effect transactions.

Owing to the physical requirements that characterized conventional businesses before the 19th century, crimes on businesses were also limited to the physical space. Hence, businesses were more exposed to crimes such as physical theft, arson, armed robbery, counterfeiting and vandalism; which most times resulted in loss of lives and properties. Consequently, businesses were protected traditionally based on both physical and procedural security measures.

However, the advent of financial technologies in the mid-19th century has significantly reduced physical crime opportunities in businesses, reduced commodity supply and demand related stress, and improved business finance accountability. The impact of financial technologies on businesses cannot be over-emphasized. For instance, the payments for goods and services have become seamless irrespective of geographical locations and time differences. Generally, financial technologies are considered indispensable in the implementation of the Central Bank of Nigeria's cashless agenda.

As a result of the tremendous benefits associated with the utilisation of financial technologies, many conventional businesses have long migrated to full fledge electronic businesses, utilising both virtual and physical spaces for sales and payments purposes. Financial technologies have contributed in no small measure in the creation of vast business opportunities via virtual markets. Products and services are now made available for customers to seamlessly pay using financial technology without necessarily carrying physical cash.

While the opportunities for physical financial crimes against businesses have been grossly reduced by the advent of financial technologies, it has however opened up new criminal opportunities via the utilization of the internet and electronic devices like the computer, smartphones, and other devices for financial transactions. Electronic businesses and their customers have oftentimes been victimised by criminals in the cyberspace.
Although ICT has impacted businesses, organisations and institutions alike, it has, however, become a breeding ground for cybercrime to thrive. Cybercriminals have become armed to steal users' information and dispossess them of their financial holdings. The trend of electronic fraud associated with the utilisation of financial technologies in electronic businesses in Nigeria has assumed a worrisome dimension and if left unchecked, could worsen as it could crumble businesses, heighten unemployment, increase the poverty rate and spike street criminality.

Despite efforts by the Central Bank of Nigeria to curtail the rate of electronic payment fraud, hardly does a day go by without individuals losing their hard-earned monies to cyber-criminals who strategically steal their financial information as they utilise electronic technologies for payments for goods and services. According to the Central Bank of Nigeria (2021), financial stability report, Point of

Sales (POS) transactions alone recorded 21.55 percent of fraud incidences. This implies a 7% rise from the previous year.

This rising electronic financial fraud does not only threaten electronic business development, it also significantly threatens individual consumers of financial technologies who may not want to utilise electronic payment channels for fear of being victimised by cyber-criminals. Consequently, the drive to a cashless economy may be hindered as individuals who develop a phobia to utilise financial technologies for transactions may still rely on physical cash.

The foregoing is a dangerous precedent not only to electronic business developments but also given the apex Bank's efforts to drive a cashless Nigerian economy. Therefore, the study seeks to investigate the specific types of cybercrimes born by the utilisation of financial technologies; how consumers of financial technologies become victims of cybercrimes; and what can be done to ameliorate the scourge of financial technology-related cybercrimes against electronic businesses.

Literature Review

Correlates of Electronic Business, Financial Technology and Cybercrime

The juxtaposition of the concepts of electronic business, financial technology and cybercrime is pertinent to the comprehension of the impact of cybercrimes on electronic business development in Nigeria. Contextually, the unfavourable criminal invention of the interplay of these three concepts under review constitutes the thesis of this article.

Electronic businesses, commonly referred to as E-Businesses entail businesses that operate on processes that are executed through any technology-mediated channel. According to the Gartner Glossary on information technology (2023), the processes involve production, customer relations and management. However, Pratt, Cole and Karjian (2022) classified electronic businesses as businesses that are executed or conducted online using the web, internet, extranet, or a combination of all. The range of activities performed in the processes of electronic businesses includes but not limited to the buying and selling of goods and services, payment processing, production and supply chain management, affiliate management, information sharing and employee services and recruitment.

According to Patrizio and Moore (2023), the term E-Business was first used by the International Business Machine Corporation (IBM) in October, 1997 in her attempt to solve the confusion customers experienced about internet-based businesses. The types of e-businesses range from business-to-business model, business to customers model, customers-to-business model, and customers-to-customers model. The term electronic business is used to describe all forms of businesses operated with the aid of financial technologies as their standard of payment (Jain, Vipin & Malviya, Bindoo& Arya, Satyendra, 2021).

Electronic businesses thrive on the altar of financial technologies. The term financial technology is utilized to imply all technological devices and software that are employed for the facilitation of business transactions about payment processing. The American Bureau of Labour Statistics (2021), described financial technology as a combination of software, mobile applications and a host of other technologies that are designed to improve and automate traditional forms of finance for businesses and their customers. This definition explicitly captures the basic rudiments of financial technology in this context.

The range of financial technologies being utilised in the world includes internet banking, credit/debit cards, and mobile money which has been proliferated with a considerably low adoption rate. For instance, mobile money has been introduced to over 90 countries in the world. These technologies aid consumers to save money, carry out transactions and have access to finance (Ligon, Malick, Sheth, and Trachtman, 2019).

Emarketer.com (2023), observed that the growth of financial technologies and electronic business is greatly challenged by the opportunities it creates for cybercriminals and financial fraudsters to perpetrate scam activities on businesses and individuals. The introduction of Financial Technology (FinTech) in the 1960s paved way for ease in various aspects of social and economic life in Nigeria. According to Okonigene & Adekanle (2010), Financial Technology as an aspect of Information and Communication Technology has facilitated connectivity, bridged physical gaps, integrated nations and made the world a global village.

The advent of the internet in 1990 proliferated the utilisation of financial technologies in different aspects of human lives, which include but are not limited to agriculture, telecommunication, education, electronic commerce, health, transportation services, Banking and Finance, etc. The financial sector is one of the most impacted as it has witnessed a significant revolution from analog to digital or electronic systems of executing financial transactions.

Ekuobase & Olutayo (2016), opined that ICT in the 21st century is a strategic asset to businesses, organisations and institutions; as it is used in the delivery of innovative services with commendable speed and accuracy. Since the emergence of the internet and other information and communication technologies, many businesses have migrated from cash payments to utilising electronic mediated means of payments like the Point of Sale (POS) machines and other applications and devices. This has precipitated a rise in the number of electronic businesses in Nigeria (Business Day, 2019).

Broby (2021) examined financial technology and the future of banking; and illustrated how financial institutions' intermediation will be impacted by innovative financial technology applications. The role of financial technologies in customer acquisition, retention and the overall enhancement of electronic business cannot be overemphasised as financial technology is best suited for intermediate roles between businesses and their customers.

Technological innovations and advancements have continued to play vital roles in the society. It has assumed an indispensable position in the affairs of man and his social existence. Emerging financial technologies has greatly revitalised the traditional analog modus operandi of various types of businesses. Financial technologies play vital roles in the handling, processing, storage, retrieval, and dissemination of information via electronic devices (Adegbija and Daramola, 2007).

Neelam and Sonali (2022) reviewed extant literature to unravel the contributions of digital technologies in financial inclusion and suggested viable directions to policymakers to further the initiatives for financial inclusion. Digital technologies were considered the drivers of financial inclusion and economic growth. This substantiates the reality of financial technologies in revolutionising business operations in Nigeria and the world at large.

Electronic devices incorporate all types of electronic-powered technologies that facilitate the financial operations and development of electronic businesses. These devices include technological

innovations handling online payment processing, electronic data exchange (EDI), inventory tracking systems, mobile commerce and automated data collection systems. Essentially, every device connected to the internet has become a functional tool in the operationalisation of electronic businesses according to its capacity.

The innovation of mobile phones accelerated the operationalisation of financial technologies. In the views of Aker and Mabiti (2010), the use of mobile phones by both urban and rural households has significantly expanded the number of consumers benefiting from the use of financial technologies, thereby, propagating electronic businesses as more and more people continue to utilise emerging financial technologies for electronic transactions.

Since the advent of financial technologies, the trend of cybercrime on electronic businesses has assumed a troubling impact. Cybercrime is a term used to describe all illicit activities that are perpetrated with the aid of internet-enabled electronic devices like the computer, smartphones and other financial technologies. The United Nations Office on Drugs and Crime (UNODC, 2023), pointed out that by way of technological abuse, cybercriminals have ruined businesses and even lives.

The World Bank (2017), disclosed that the basic threat to financial technology utilisation is the basis that approximately 2.5 billion potential financial technology consumers do not hold financial accounts. However, mobile payment is still one of the most widely utilised financial technologies for digital payments and communications. Despite this, there is low patronage of financial technologies due to cyber or electronic fraud (Broby, 2021).

Stijn (2006) observed that most countries do not give priority to policy formulations that support universal access to financial services. Therefore, the need to facilitate access to financial services can be achieved by strengthening institutional infrastructure, liberalizing markets, facilitating competition and encouraging innovative utilisation of technological know-how. Additionally, policies must meet the primary considerations of financial technology consumers, which include cost reduction, convenience, and real-time data tracking for decision-making.

Cybercrime and Electronic Business Development

The adoption and utilization of financial technologies in electronic businesses have gained significant traction as it provides access to global markets, offer competitive advantages and increase the effectiveness of businesses (Apau, Koranteng & Gyamfi, 2019). However, electronic businesses and their customers have continued to suffer losses from the activities of cybercriminals who trail and prey on electronic business activities and processes with the ultimate aim of attracting illicit financial benefits.

Duah and Asirifi (2015), investigated the impact of cybercrime on the development of electronic business in Ghana, and discovered that cyber-fraud had direct financial losses to consumers and businesses because websites suffer spoofing and hijacking, payment systems can be compromised and funds can be transferred at a speed of light. They observed that these electronic crimes result in consumers' tremendous phobia of venturing into electronic financial transactions and have heightened privacy concerns about public utilization of financial technologies. Therefore, the pace of electronic business development is limited by consumers' fears of being victimized by cybercriminals.

In another study conducted by Apau and Koranteng (2019) on the impact of cybercrimes and trust on the use of e-commerce technologies, the lack of trust in internet media, subjective norms and

perceived external usability control are deterrents to the utilisation of financial technologies. The obvious lack of trust corroborates the fears exercised by consumers of financial technology, thereby, necessitating the continuous internalisation of the conventional face-to-face economic life of individuals. This further strengthens the position that if electronic businesses are to assume the normal pace of development, then the issue of trust in the utilisation of financial technologies must be addressed by implementing measures that will curb cybercrimes on electronic businesses.

Similarly, Jabar (2022) examined individuals' perception and the usage of e-commerce business technology platforms in Lagos Metropolis, Nigeria and found that the utilisation of e-commerce technologies was adversely affected by the negative perception of cybercrimes on e-businesses. This underscores the need for comprehensive cyber law enactments and the deployment of adequate cyber security systems to guarantee users' protection and safety.

Some Common Types of Financial Technology-Enabled Cybercrimes

The advent of ICT, particularly financial technologies, birthed criminal prospects that are bedevilling the going concern of many electronic businesses (Ashibi, 2021). These criminal prospects are perpetrated in diverse ways unknown to vendors and their consumers. Rafael (2023), outlined the types of cybercrimes that are associated with electronic businesses including but not limited to the followings:

a. **Credit card fraud:** This relates to all types of fraud that are committed with the aid of a credit card. Credit cards are often stolen by the fraudster to transact electronically without the approval of the actual owner. An instance of this is the purchase of credit cards in the dark web or black market by cybercriminals and utilising such cards to purchase goods and services electronically. Although, the cardholder may be debited in the long run, the merchant who sold such goods or services will bear the burden of such loss as they have to make refunds to the actual cardholder. According to Ashibi (2021), this type of electronic financial fraud is associated with the utilisation of credit and debit cards financial technologies.
b. **Affiliate Fraud:** This type of electronic fraud is common in affiliate marketing. Here, the cybercriminals compromise the merchant's online stores and defraud the merchant by fraudulently generating sales activities with the ultimate aim of increasing the commission due to them. It is common to find this type of electronic fraud particularly on electronic payment gateways of merchants. Cybercriminals take advantage of payment gateway technologies to actualize their criminal motives on electronic businesses.
c. **Chargeback Fraud:** This is a situation where a payment service provider demands a merchant to make a refund for a transaction that is assumed fraudulent or disputed. Cybercriminals take advantage of this window to request a financial refund from their merchants via the payment service providers on the criminal claim that their orders were not successfully delivered but were debited. Typically, the fraudster makes an online purchase, receives the order(s), and deliberately waits for weeks or months before making a refund claim to their bank on the basis that the transaction was fraudulent or unauthorised.
d. **Phishing:** This is the unauthorised access to customers' financial accounts or wallets as may be created by online merchants and financial institutions. Online fraudsters use phishing schemes to hack into these accounts and carry out illicit transactions. Oftentimes, the actual account owners are tricked by emails or phone calls to reveal their personal information which will aid the fraudsters to gain access to their accounts. These personal information may include usernames, passwords, Personal Identification Number (PIN), etc. Technologies such as the internet, digital computers, mobile phones and technology-mediated communication

channels (like emails, SMS, etc) are veritable tools in the hands of cybercriminals in perpetrating phishing activities (Ashibi, 2021).

e. **Intercept fraud:** This involves the tactics of utilizing stolen credit cards to initiate electronic transactions, and make payments but intercepts the delivery before the products or services are delivered to the address identified on the credit card. A good example of this in Nigeria is a situation where a cybercriminal places an order on Jumia, but after the order, calls the company to change the delivery address. This diversion is what is termed intercept fraud.
f. **Triangulation fraud:** This is a complex type of financial fraud where the cybercriminal considers three steps. Summarily, the fraudster squat under popular brand names to create online stores with the ultimate aim of stealing credit card details. The stolen credit card details are used to order products or services without authorisation from the actual owner of the card.

Theoretical Framework

Given the fast pace of the internet revolution which is sweeping across the globe with a juxtaposition of its concomitant impetus to an array of financial technologies, traditional ways of doing business and mode of payments have been significantly altered. Consequently, businesses and individuals are increasingly adapting to the digital or electronic culture of utilising electronic devices and internet technologies in carrying out daily transactions.

The space transaction theory is employed to expressly elucidate how the transition from the physical or manual ways of doing business to the contemporary digital culture of electronic business operation has impacted crime and criminal victimization. The internet evolved with new forms of deviance, crime and social control measures. These new realities in the cyberspace have become immediate threats to electronic businesses.

The space transition theory was developed by Jaishankar K. in 2008. It is a theory of cybercrime which expresses how the cyberspace has emerged as a fertile ground for criminal activities to thrive. This theory explains the conforming and non-conforming behavioural differences of people in the physical space and when they transit to the cyberspace (Jaishankar, 2008). The theory holds that individuals who ordinarily would not venture into criminality in the physical space because of their social status and position may do so in the cyberspace because of its potential for anonymity. This is because the cyberspace has identity flexibility, dissociative anonymity and a lack of deterrence factors. Besides, cybercrime thrives on the virtue that criminals can escape easily because cyberspace location can be seamlessly changed as the offender can move from one space to another.

This theory is relevant to the extent that it explains how electronic crimes are exacerbated by the anonymity and flexibility embedded in the cyberspace. Therefore, the cyberspace has become the new "Heaven" for criminals in the physical space to migrate their illicit tendencies. It further portrays the fact that individuals who because of their social statuses in the society would not want to commit crime in the physical space, now have an opportunity in the cyberspace to take advantage of the elements of flexibility and anonymity of the cyberspace to commit electronic or cybercrimes. This theory adequately accounts for the proliferation of cybercrimes in electronic businesses today.

Methodology

The Research Design

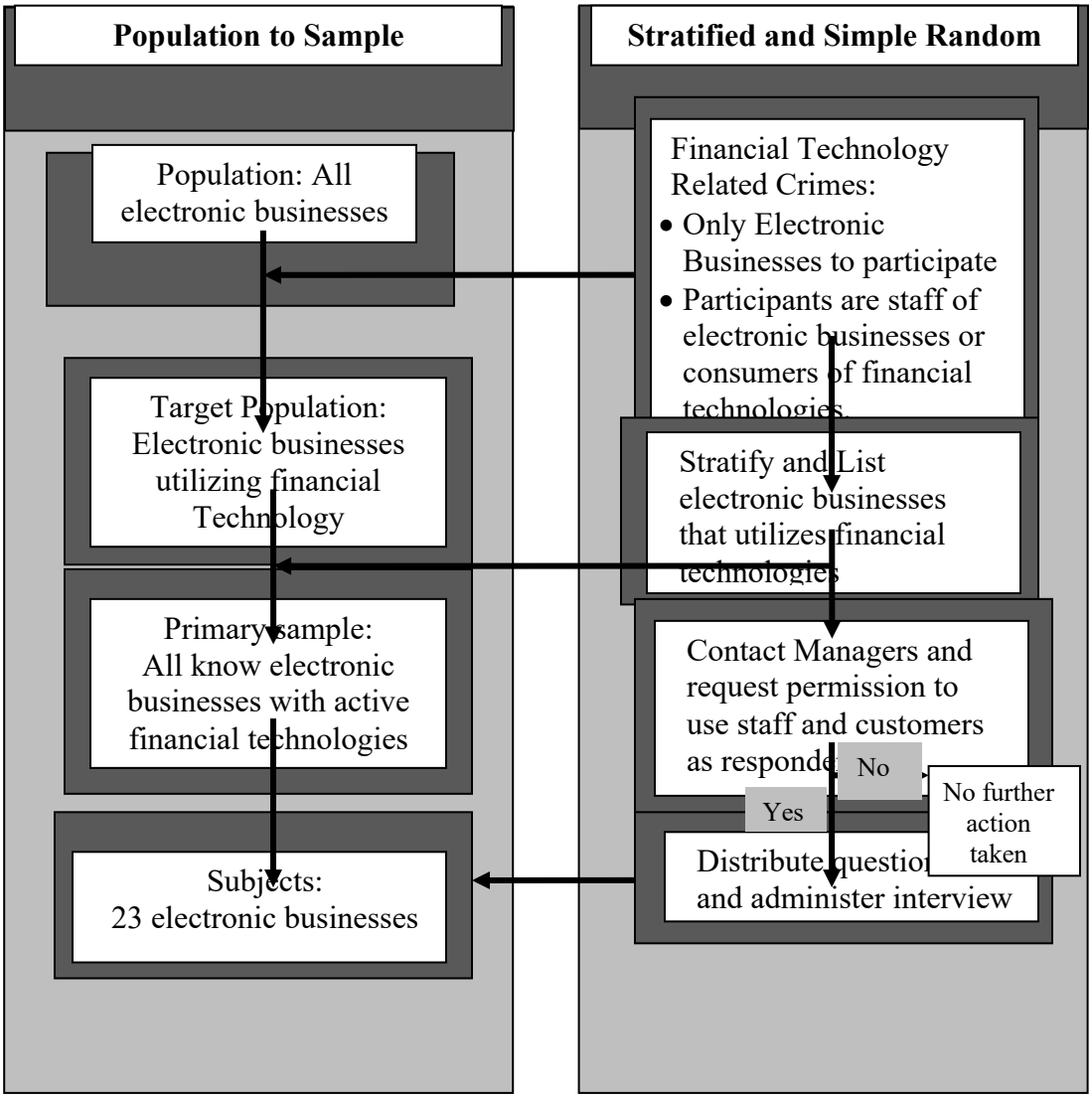
The case study approach was adopted to critically examine the behavioural pattern of financial technology utilisation by electronic businesses and their consumers. Essentially, data for the study were elicited from the respondents using a well-structured questionnaire as the main instrument of data collection. Data collated from the questionnaires were analysed with the aid of the Statistical Package for the Social Sciences (SPSS) to identify and establish prominent patterns among consumers of financial technology and electronic businesses.

The case study design is a highly practicable research method as it is of immense help in contributing to exposing the common types of financial fraud associated with electronic businesses in Nigeria. However, the need to triangulate with the descriptive research design was found to be appropriate in the collation, analysis and presentation of the quantitative research data. This gave room for us to provide insight into answering the questions of the "why" and "how" of cybercrimes on electronic businesses via financial technologies in Nigeria.

Sampling Techniques

The probability and non-probability sampling techniques were adopted in selecting the required respondents for the study. The probability sampling method that was employed is the stratified and simple random sampling techniques, while the purposive and snowball sampling techniques were the non-probability sampling methods. Ikeja Local Government Area of Lagos State was delineated according to its 12 districts or communities (Anifowose, Oregun, Ojodu, Opebi, Akiode, Alausa, Agidingbi, Ogba, Magodo, Maryland, Onigbongbo and the Government Reserve Area). Each district was stratified based on major electronic business locations. To avoid bias in the selection process, the simple random sampling technique was utilised to draw samples from the various strata in such a way that the different units in the population of the study had equal chances of being selected. Finally, the purposive and snowball sampling techniques were deployed to identify and administer the research instruments to the respondents.

Figure 1: Sampling procedure from population to sample



Source: Developed by the researchers, 2023.

Cronbach's Alpha Reliability of the Research Instruments:

$$\alpha = \frac{\bar{N}\bar{c}}{\bar{v} + (N-1)\bar{c}}$$

Table 1: Cronbach's Alpha for measurement of scale reliability for the Research Instruments

Instrument sub-focus	Cronbach's alpha	No of Items
Types of electronic businesses	.876	4
Characteristics of electronic businesses	.821	3
Staff	.732	63
Managers	.895	23
Customers	.865	93
Use of financial technologies	.829	23
Financial technology service providers	.764	6
Fraud on electronic businesses	.983	12
Types of electronic business fraud	.854	6
Causes of electronic business fraud	.833	9
Impact of electronic business fraud	.822	6
Confidence on electronic business	.867	4
Solutions to electronic business fraud	.726	6

Source: Fieldwork, 2023.

Findings and analysis

Findings are presented thematically based on the research objectives that were addressed by the relevant sections of the research questionnaire and interview guide that were administered to the respondents of the study. Simple statistical tables were employed for the presentation of the quantitative data elicited from the respondents.

Table 2: Financial Technology Utilization Preferences

Fintech. Service Providers	Yes	No	Neutral	Total
Flutterwave	8 (35%)	13 (56%)	2 (9%)	23 (100%)
Paystack	14 (61%)	8 (35%)	1 (4%)	23 (100%)
Accelerex	9 (39%)	3 (13%)	11 (48%)	23 (100%)
PiggyVest	7 (30%)	2 (9%)	14 (61%)	23 (100%)

Paga	11 (48%)	4 (17%)	8 (35%)	23 (100%)
Interswitch	12 (52%)	5 (22%)	6 (26%)	23 (100%)
E-transact	11 (48%)	8 (35%)	4 (17%)	23 (100%)
Carbon Paylater	6 (26%)	2 (9%)	15 (65%)	23 (100%)
Remita	15 (65%)	2 (9%)	6 (26%)	23 (100%)
Kuda	9 (39%)	3 (13%)	11 (48%)	23 (100%)

Source: Fieldwork, 2023.

Table 2 above indicates the utilisation preference of some major financial technology service providers in the study area. The table revealed that most consumers utilising financial technologies prefer Remita (65%), Paystack (61%) and Interswitch (52%) over other payment service providers. However, Paga (48%), E-transact (48%), Accelerex (39%), and Flutterwave (35%) were considered the most viable alternatives. Hence, consumers' preference for these payment service providers is assumed to be based on transaction transparency, swift dispute resolution, and low-cost processing fees.

Table 3: Challenges Facing Financial Technology Utilisation
Legend *- 1 = Very Severe 2 = Severe 3 = Neutral 4 = Less severe 5 = Not severe*

Variables	1	2	3	4	5	Mean	Rank
High transaction service cost	32.1	16.4	-	-	-	3.65	7th
Electronic financial fraud	73.5	25.9	-	-	-	4.95	1st
Service/Network downtime	45.2	17.2	-	-	-	4.65	3rd
Delays in credit/debit	65.8	21.6	-	-	-	3.99	5th
Lack of financial privacy	50.6	18.2	-	-	-	3.87	6th
Lack of transparency	25.9	12.3	22.5	-	-	4.60	4th
Harmful manipulation	73.1	25.9	-	-	-	4.88	2nd
Others	-	-	-	-	-	-	-

Source: Fieldwork, 2023.

Table 3 above represents an analysis of the respondents' responses on the various limitations on the utilisation of financial technologies. Results from the analysis revealed that most respondents (represented by a mean value of 3.65) are apprehensive about utilising financial technologies due to their susceptibility to electronic fraud. From the result, the issue of financial fraud is considered very severe as it has become a major impediment for most consumers of financial technologies to utilise the option as a means of carrying out financial transactions. Besides, the majority of the respondents further allured to the position that transactions carried out via financial technologies are prone to harmful manipulations (represented by a mean value of 4.88). This challenge is considered severe. However, the challenge of lack of transparency in transactions via financial technologies was downplayed by most of the respondents as they chose to remain neutral (represented by a mean value of 4.68). Whereas, delays in credit/debit (3.99), lack of financial privacy (4.60) and high transaction service cost (3.65) were not considered severe impediments to the use of financial technologies.

Table 4: Types of cybercrimes/fraud associated with financial technologies
Legend: SA=Strongly Agreed; A=Agreed; UD=Undecided; D=Disagreed; SD=Strongly Disagreed

S/N		% Rating					Mean	STD
	Fraud types	**SA**	**A**	**UD**	**D**	**SD**		
1.	Triangulation fraud	43.9	42.3	1.5	3.8	3.4	4.24	1.050
2.	Identity theft	41.9	45.2	2.7	6.6	4.6	4.11	0.958
3.	Credit card fraud	39.2	38.1	0.5	5.3	7.5	4.15	1.166
4.	Affiliate fraud	32.8	34.9	6.2	13.5	12.6	3.62	0.898
5.	Phishing	37.6	45.9	0.7	2.3	3.7	4.31	1.386
6.	Intercept fraud	43.4	39.0	3.2	10.7	13.7	3.68	1.020
7.	Chargeback fraud	42.2	42.9	3.7	3.4	5.0	4.19	1.388

Source: Fieldwork, 2023.

Findings from the field with regard to the types of cybercrimes or electronic fraud associated with financial technologies are presented in Table 4 above. The respondents' ratings on the most prevalent types of electronic financial fraud reveal triangulation fraud, identity theft, credit card fraud, affiliate fraud, phishing, intercept fraud and chargeback as the most common types of electronic fraud associated with financial technologies.

The respondents' ratings on the types of electronic fraud reveal a statistically significant correlative pattern on triangulation fraud, identity theft, credit card fraud, phishing, and chargeback with mean scores of 4.24, 4.11, 4.15, 4.31 and 4.19 respectively. These frauds are tagged as the most prevalent types of fraud in the study area. However, other types of electronic fraud like intercept and affiliate frauds are also present in financial technologies but their impacts are not felt significantly yet.

Discussion

The advent of financial technologies has established a fertile ground for electronic financial fraud to thrive. Hence, this study set out to examine the types of cybercrimes/electronic fraud that are associated with financial technologies and their effects on the utilization of financial technologies for electronic transactions. Therefore, the findings from the study are discussed thematically as follows:

As indicated in Table 2, the study revealed that Remita (65%), Paystack (61%) and Interswitch (52%) are the most preferred financial technologies utilised by consumers. This result is largely based on transparency, dispute resolution and cost of processing fees. It entails that users' preference for financial technologies is a reflection of their direct experience or on the shared experiences of others about convenience and other benefits. This corroborates the position of Stijn (2006), who stated that the primary considerations of financial technology consumers include cost reduction, convenience, and real-time data tracking for decision-making.

Furthermore, findings from the study as presented in Table 3 revealed the major challenges facing financial technology utilisation. Among these challenges are high transaction service cost(7th), electronic financial fraud(1st), service/network downtime(3rd), delays in credit/debit(5th), lack of financial privacy(6th), lack of transparency(4th) and harmful manipulation(2nd). These challenges possess as impediments to the utilisation of financial technologies for electronic transactions. However, electronic financial fraud was identified as the most severe challenge hampering financial technology consumers from utilising financial technologies in electronic transactions. This finding clearly explains why most persons chose to transact with physical cash even when they were issued instruments of financial technologies like credit/debit cards, online financial applications, etc. This finding is supplemented by the views of Apau and Koranteng (2019) on the lack of trust in the utilisation of financial technologies. Individuals or financial technology consumers are apprehensive because they or others have at one point or another suffered financial loss(es) as a result of utilising financial technologies.

Finally, Table 4 indicates the respondents' responses on the types of cybercrimes/fraud associated with financial technologies. Although, it was gathered that triangulation fraud, identity theft, credit card fraud, affiliate fraud, phishing, intercept fraud and chargeback are all evident in financial technologies, however, triangulation, phishing, identity theft and credit card fraud were identified as the most prevalent types of cybercrime or electronic fraud associated with financial technology utilisation in the study area. By implication, these electronic financial frauds are the major threats to financial technology utilisation by consumers. This finding is in line with the views of Broby (2021) who posited that there is low patronage of financial technologies due to cyber or electronic fraud inherent in financial technology loopholes that have been taken advantage of by cybercriminals. Therefore, to up users' utilisation, concerted efforts must be made by stakeholders of digital financial technologies to close the loopholes to curb these electronic frauds, especially given the Apex Bank's (Central Bank of Nigeria) economic decision to migrate to a full-fledged cashless economy.

Conclusion and Recommendations

Because of the fast-transitioning pace of Nigeria's digital economy, it is imperative to examine the utilisation of financial technologies with the primary aim of unravelling its basic threats and proffering feasible measures to curb such threats. Financial technology has continued to remain indispensable in the electronic commerce industry. For instance, major electronic commerce players in Nigeria like Jumia International, Zikel Cosmetics, Soso Games, SLOT Systems Limited, and other electronic businesses, utilises financial technologies through financial technology service providers like Paystack,

Remita, E-transact, Paga, Interswitch, etc for basic financial operations or transactions. Therefore, the advent of financial technology has revolutionised the physical marketplace into a virtual global market with ease of transaction and communication between vendors and clients.

Converse to the successes of financial technologies in electronic commerce, cybercriminals have found it a fertile terrain to defraud unsuspecting users and dispossess them of their financial worth and valuables. This criminal aim of financial fraudsters is perpetrated via acts of triangulation fraud, identity theft, credit card fraud, affiliate fraud, phishing, intercept fraud, chargeback and other means of electronic financial fraud.

Consequently, this study examines financial technology utilisation in electronic businesses with the primary aim to determine such factors responsible for low patronage from individuals and businesses. Based on the findings of the study, the following recommendations are made to curb the trend of financial fraud exacerbated by financial technology and to encourage its utilisation by individuals and businesses.

i. As the apex bank, the Central Bank of Nigeria should exercise deliberate and decisive efforts in promoting awareness to up consumers' financial technology literacy to boost its utilisation and avoid victimisation by cyber criminals.
ii. Government should criminalise all acts of financial fraud including the intent or attempts to do so. This can be achieved by adequate policy formulation and enforcement to punish and deter potential cyber-criminals.
iii. Law enforcement agents should be empowered appropriately to investigate and arrest the litany of financial fraudsters who utilise traceable technology-mediated communication channels (like mobile phones, emails, etc) to perpetrate the crimes.
iv. Relevant financial regulatory bodies and authorities like the Central Bank of Nigeria, should strive for policies that will compel financial institutions to upgrade their financial technologies to incorporate Europay, MasterCard and Visa (EMV) Chip and Near Field Communication (NFC) technologies. These are globally recognised technological components with high-level security to protect the users.

References

Adegbija, M. V. & Daramola, F. O. (2007). Evaluation of computer education in higher institutions in Ilorin South Local Government. African Journal of Educational Studies. (AJES). 4(11).

Aker, J. C., & Mbiti, I. M., 2010. Mobile phones and economic development in Africa. Journal of economic Perspectives, 24(3), 207-32. DOI: 10.1257/jep.24.3.207

Apau, R., and Koranteng, F. (2019). Impact of Cybercrime and Trust on the use of E-Commerce Technologies: An Application of the Theory of Planned Behavior. International Journal of Cyber Criminology - ISSN: 0974-2891. 13(2). DOI: 10.5281/zenodo.3697886

Apau, R., Koranteng, F., & Gyamfi, S. (2019). Cyber-Crime and its Effects on E-Commerce Technologies. Journal of Information, 5(1), 39–59. https://doi.org/10.18488/journal.104.2019.51.39.59

Ashibi, J. E. (2021). Influence of Technology-Mediated Communication Channels on Cybercrimes. A Study of ICT users in the Southern Senatorial District of Cross River State, Nigeria. Journal of Sociology. Osun State University. Vol.7.1

Broby, D. (2021). Financial Technology and the Future of Banking. Financial Innovation, SpringerOpen, United Kingdom.

Bureau of Labour Statistics (2021). Financial Analysts. The Fu Foundation School of Engineering and Applied Science. Available at: https://bootcamp.cvn.columbia.edu/blog/what-is-fintech/. Accessed June, 2023.

Business Day (2019). Growth of Digital Businesses in Nigeria. Available at: https://businessday.ng/editorial/article/growth-of-digital-businesses-in-nigeria/

Duah, F. and Asirifi, M. (2015). The Impact of Cybercrime on the Development of Electronic Business in Ghana. European Journal of Business and Social Sciences, Vol. 4(1). ISSN: 2235-767X

Ekuobase O. and Olutayo A. (2016). Study of information and communication technology (ICT) maturity and value: The relationship. Egyptian informatics journal, Vol. 17, Pg 239-249.

Gartner Glossary on information technology(2023). E-Business. Available at: https://www.gartner.com/en/information-technology/glossary/e business#:~:text=E%2DBusiness%20(electronic%20business),%2C%20governmental%2C%20or%20nonprofit%20entity.

Jabar, A. (2022). Cybercrimes Perception and Usage of E-Commerce Business Technology Platforms in Lagos Metropolis, Nigeria. Journal of Research in Business and Management. 10(6) pp58-64. Available at: https://www.questjournals.org/jrbm/papers/vol10-issue6/Ser-3/I10065864.pdf

Jain, Vipin and Malviya, Bindooand Arya, Satyendra (2021). An Overview of Electronic Commerce (e-Commerce). Journal of Contemporary Issues in Business and Government. 27. 665-670. 10.47750/cibg.2021.27.03.090.

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Ligon, E., Malick, B., Sheth, K. and Trachtman, C., 2019. What explains low adoption ofdigital payment technologies? Evidence from small scale merchants in Jaipur, India. PloSone, 14(7), p.e0219450.https://doi.org/10.1371/journal.pone.0219450

Neelam, Km. and Bhattacharya, Sonali, Financial Technology Solutions for Financial Inclusion: A review and future agenda, Australasian Accounting, Business and Finance Journal, 16(5), 2022, 170-184. doi:10.14453/aabfj.v16i5.11

Nigeria Inter-Bank Settlement System (NIBSS) 2021 Annual Financial Stability Reports. Retrieved from: https://nibss-plc.com.ng/stability-report.

Okonigen. R. and Adekanle, B. (2010). Cybercrime in Nigeria. Business Intelligence Journal. Vol. 3 (1): 1 – 6.

Patrizio, A. and Moore, J. (2023). International Business Machine Corporation (IBM). Available at: https://www.techtarget.com/searchitchannel/definition/IBM-International-Business-Machines. Accessed on July, 2023.

Pratt, M., Cole, B. and Karjian, R. (2022). The Evolving CIO Role: From IT Operator to Business Strategist. Available at: https://www.techtarget.com/searchcio/definition/e-business . Accessed June, 2023.

Rafael L. (2023). Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide. Available at: https://www.bigcommerce.com/blog/ecommerce-fraud/. Accessed April, 2023.

Stijn, C. (2006). Access to Financial Services: A Review of the Issues and Public Policy Objectives. The World Bank Research Observer, 21.2. 207-240.

UNODC, (2023). University Module Series on Cybercrime. Available at: https://www.unodc.org/e4j/en/tertiary/cybercrime.html. Accessed: July, 2023.

World Bank (2017). The Global Findex Database 2017. https://globalfindex.worldbank.org/